

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problems Mailbox.**

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-204955

(43)Date of publication of application : 09.08.1996

(51)Int.Cl. H04N 1/40
G03G 21/04
G03G 21/00

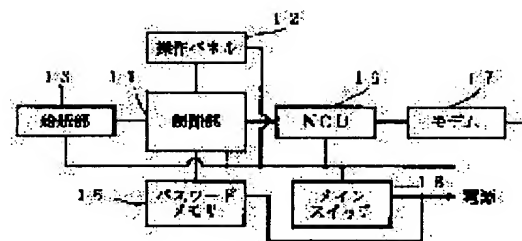
(21)Application number : 07-011066 (71)Applicant : MITA IND CO LTD

(22)Date of filing : 26.01.1995 (72)Inventor : YAMASHITA YUJI

(54) COPYING MACHINE MANAGEMENT DEVICE**(57)Abstract:**

PURPOSE: To provide a copying machine management device which can prevent the forgery of the paper moneys, the securities, etc., by preventing the production of copies performed by a copying machine that is improperly transported by theft, etc.

CONSTITUTION: The power is supplied to a copying machine control part 11, a control panel 12, a paper feed part 13, an NCU 16, a modem 17, etc., of a copying machine management device via a main switch 18. When the main switch of a copying machine is turned on, the password that is collated with the password supplied from the outside is stored in a password memory 15. The memory 15 is connected to a password memory power supply part which is backed up with no intervention of the switch 18 only when a power cable is connected to a prescribed power supply part.

**LEGAL STATUS**

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2000 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平8-204955

(43) 公開日 平成8年(1996)8月9日

(51) Int.Cl. ⁶	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 N 1/40				
G 0 3 G 21/04				
21/00	3 9 6			
			H 0 4 N 1/ 40	Z
			G 0 3 G 21/ 00	3 9 0
			審査請求 未請求 請求項の数 3	OL (全 6 頁)

(21) 出願番号 特願平7-11066

(22) 出願日 平成7年(1995)1月26日

(71) 出願人 000006150

三田工業株式会社

大阪府大阪市中央区玉造1丁目2番28号

(72) 発明者 山下 裕司

大阪市中央区玉造1丁目2番28号 三田工業株式会社内

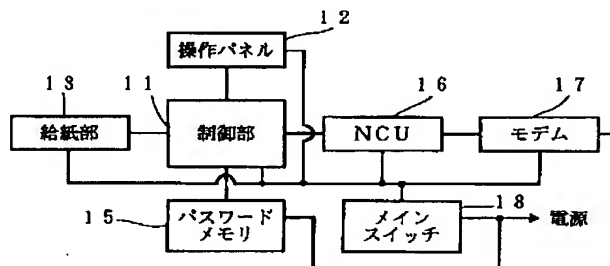
(74) 代理人 弁理士 小野 由己男 (外1名)

(54) 【発明の名称】 複写機管理装置

(57) 【要約】

【目的】 盗難等により不当に移動された複写を用いて複写物を作成することを防止し、紙幣や有価証券等の偽造を未然に阻止することにある。

【構成】 複写機管理装置は、複写機の制御部11、操作パネル12、給紙部13、NCU16及びモデム17等の各部にメインスイッチ18を介して電源供給を行っている。複写機のメインスイッチがオンされたときに、外部から入力されるパスワードと照合されるユーザパスワードがパスワードメモリ15に格納されている。このパスワードメモリ15はメインスイッチ18を介さずに、電源ケーブルが所定の電源部に接続されているときのみ電源バックアップされるようなパスワードメモリ用電源部に接続されている。



【特許請求の範囲】

【請求項1】揮発性の記憶手段で構成され、ユーザパスワードを記憶するパスワードメモリと、
複写機のメインスイッチがオンされると、パスワード入力を要求するパスワード要求手段と、
外部から入力されるパスワードを受け付けるパスワード受付手段と、
前記パスワード受付手段により受け付けられたパスワードを、前記パスワードメモリに記憶されているユーザパスワードと照合し、合致していれば複写動作の許可を行うパスワード照合手段と、
複写機の電源ケーブルが所定の電源部に接続されているときのみ、前記パスワードメモリに電源バックアップを行うパスワードメモリ用電源部と、を備える複写機管理装置。

【請求項2】複写機を管理するホストコンピュータと回線を介して接続され、前記パスワードメモリは、前記ホストコンピュータにより設定されるユーザパスワードを記憶する、請求項1に記載の複写機管理装置。

【請求項3】前記複写機は、前記ホストコンピュータに通信を行いパスワード設定要求を行うパスワード設定要求手段をさらに備え、

前記ホストコンピュータは、前記複写機の回線番号を記憶する記憶手段と、前記パスワード設定要求に基づいて、前記記憶手段から複写機の回線番号を読み出して通信を行う通信手段と、前記通信手段からの通信が正常に行われたとき、前記パスワード設定要求が正当な要求であると判断し、前記ユーザパスワードを送信するパスワード設定手段とをさらに備える、請求項2に記載の複写機管理装置。

【発明の詳細な説明】**【0001】**

【産業上の利用分野】本発明は複写機管理装置に関する。

【0002】

【従来の技術】複写機、特にカラー複写機では、紙幣や有価証券等の偽造を防止することに配慮する必要がある。たとえば、複写物に当該複写機のモデル番号やシリアルナンバー等を印刷することにより、コピーを行った複写機を特定し、そのユーザを特定できるように構成された複写機が存在している。

【0003】

【発明が解決しようとする課題】このような複写機においては、偽造された紙幣や有価証券等に印刷されたシリアルナンバーから利用された複写機を割り出すことは可能である。しかしながら、盗難等により複写機が不当に移動された場合には、偽造を行った犯人の特定をすることは不可能である。

【0004】本発明は、盗難等により不当に移動された複写機を用いて複写物を作成することを防止し、紙幣や

有価証券等の偽造を未然に阻止することにある。

【0005】

【課題を解決するための手段】本発明に係る複写機管理装置は、パスワードメモリと、パスワード要求手段と、パスワード受付手段と、パスワード照合手段と、パスワードメモリ用電源部とを備えている。パスワードメモリは揮発性の記憶手段で構成され、ユーザパスワードを記憶する。パスワード要求手段は複写機のメインスイッチがオンされるとパスワード入力を要求する。パスワード受付手段は外部から入力されるパスワードを受け付ける。パスワード照合手段は、パスワード受付手段により受け付けられたパスワードを、パスワードメモリに記憶されているユーザパスワードと照合し、合致していれば複写動作の許可を行う。パスワードメモリ用電源部は、複写機の電源ケーブルが所定の電源部に接続されているときのみ、パスワードメモリに電源バックアップを行う。

【0006】複写機を管理するホストコンピュータと回線を介して接続され、パスワードメモリがホストコンピュータにより設定されるユーザパスワードを記憶する構成とすることができる。複写機が、ホストコンピュータに通信を行いパスワード設定要求を行うパスワード設定要求手段をさらに備え、ホストコンピュータが複写機の回線番号を記憶する記憶手段と、パスワード設定要求に基づいて、記憶手段から複写機の回線番号を読み出して通信を行う通信手段と、通信手段からの通信が正常に行われたとき、パスワード設定要求が正当な要求であると判断し、ユーザパスワードを送信するパスワード設定手段とをさらに備える構成とすることができる。

【0007】

【作用】本発明に係る複写機管理装置では、複写機のメインスイッチがオンされると、パスワード要求手段によりパスワード入力を要求し、パスワードの入力を受け付ける状態となる。このときパスワード受付手段により外部から入力されるパスワードを受け付けると、パスワード照合手段によりパスワードメモリに記憶されているユーザパスワードとの照合を行う。このパスワード照合手段による照合が合致している場合には複写動作の許可を行う。ユーザパスワードを記憶しているパスワードメモリは、複写機の電源ケーブルが所定の電源部に接続されているときのみ電源バックアップが行われており、複写機が移動されて電源ケーブルが外されると、パスワードメモリ内に格納されているユーザパスワードが消滅するように構成されている。

【0008】ホストコンピュータと回線を介して接続されている複写機の場合には、ホストコンピュータにより設定されるユーザパスワードをパスワードメモリによって記憶するように構成できる。したがって、停電やその他の状況で複写機の電源ケーブルが所定の電源部から切り離された場合には、ホストコンピュータから新たなユ

ーザパスワードを設定し、正当なユーザによる使用が可能となる。

【0009】複写機がパスワード設定要求手段を備え、ホストコンピュータが記憶手段と通信手段とパスワード設定手段とを備える構成とした場合には、複写機からのパスワード設定要求があったとき、ホストコンピュータ側から複写機の回線番号に通信を行って、正常な通信が行われたときに、ユーザパスワードの設定を行うように構成でき、高いセキュリティを維持することができる。

【0010】

【実施例】本発明に係る複写機管理装置の一実施例を図に基づいて説明する。図1に示すように複写機1は、公衆回線2を介してホストコンピュータ3に接続されている。図示したように、ホストコンピュータ3が複数の複写機1、1を管理するように構成することができる。複写機1は、原稿を読み取るための露光部、読み取った原稿のトナー画像を形成するための画像形成部、画像形成部へ用紙を供給する給紙部、画像形成部で用紙に形成された画像を加熱定着する定着部等を有している。

【0011】さらにこの複写機1には図2に示す制御部11が設けられている。制御部11は、CPU、RAM、ROM、各種ドライバ及びI/Oを含むマイクロコンピュータシステムで構成されている。制御部11には、操作パネル12が接続されている。操作パネル12は複写機本体の上面に配置されており、入力キー部及び液晶表示素子またはLED等で構成される表示部を含んでいる。制御部11にはさらに、装着される給紙カセットやバイパステーブル等から画像形成部へ用紙を供給する給紙部13が接続されている。

【0012】また、制御部11には、ユーザパスワードを記憶するパスワードメモリ15が接続されている。制御部11は、さらにネットワーク制御ユニット（以下NCUと称す）16及びモデム17を介して公衆回線2に接続される。制御部11、操作パネル12、給紙部13、NCU16及びモデム17には、メインスイッチ18を介して電源部が接続されている。パスワードメモリ15は、メインスイッチ18を介さずに電源部が直接接続されている。

【0013】ホストコンピュータは、図3に示すようにCPU21と、CPU21に接続されるRAM22、ROM23及び入出力インターフェイス24とを含む。このCPU21には、表示用のCRT25、入力用キーボード26、記憶装置28等も接続されている。記憶装置28はたとえば、ハードディスク等で構成されており、公衆回線を介して接続されている各複写機1、1の回線番号を記憶する領域が設けられている。入出力インターフェイス24にはRS232C等の入出力端子が設けられており、通信用のモデム27を介して公衆回線2に接続されている。

【0014】次に上述の実施例の動作を説明する。

複写機

複写機1は、図4に示すような動作を行う。複写機1のメインスイッチが投入されると、ステップS1において各種パラメータを初期化する。ここでは、パスワード入力回数を計数するための変数kを“0”にリセットする。ステップS2では、パスワードメモリ15内にユーザパスワードが記憶されているか否かを判断する。パスワードメモリ15内にユーザパスワードが記憶されている場合には、ステップS3に移行する。ステップS3では、操作パネル12の表示部に、ユーザに対してパスワード入力を促す表示を行う。ステップS4では、ユーザによるパスワードの入力が行われたか否かを判断する。ここでは、操作パネル12に設けられている入力キー部からのパスワード入力を受け付ける。ユーザによるパスワード入力を受け付けたときには、ステップS5に移行する。ステップS5では、パスワード入力回数を示す変数kをインクリメントする。

【0015】ステップS6では、ステップS4で入力されたパスワードとパスワードメモリ15に格納されているユーザパスワードとを照合し、一致しているか否かを判断する。ステップS6においてパスワードが一致していると判断したときには、ステップS7に移行する。ステップS7では、通常のコピー動作が可能となるように、定着部を所定の温度に制御する等のコピー動作準備処理を行う。ステップS8では、操作パネル12の入力キー部が操作されてコピー動作が指示されたか否かを判断する。コピー動作が指示された場合には、ステップS9に移行する。ステップS9では、ステップS8で受け付けた操作に応じてコピー動作を行う。ステップS10では他の処理を行う。ステップS11ではメインスイッチがオフされたか否かを判断する。複写機1のメインスイッチがオフされていない場合には、ステップS8に移行する。ステップS11でメインスイッチがオフされると処理を終了し、各部への電源供給をオフする。

【0016】ステップS6において、パスワード照合が一致しないと判断した場合には、ステップS12に移行する。ステップS12では、パスワード入力回数を示す変数kを所定の値nと比較する。所定の値nは、パスワード入力回数がこの値を超えたときに、パスワードメモリ15内のユーザパスワードを無効にするためのしきい値であり、たとえば“3”に設定される。変数kが所定の値nを下回る値であれば、ステップS3に移行する。ステップS12で、変数kの値が所定の値nと同じかそれを超える値となったと判断すると、ステップS13に移行する。ステップS13では、パスワードメモリ15に格納されているユーザパスワードを消去する。この後複写機1の処理を終了する。

【0017】ステップS2においてパスワードメモリ15内にユーザパスワードが記憶されていないと判断した場合にはステップS14に移行する。ステップS14で

は、操作パネル 12 の表示部に、ユーザに対してパスワード設定要求を促す表示を行い、ユーザによる初期設定を行うか否かの入力待ちを行う。ステップ S 15 ではユーザによる初期設定を行う旨の入力があったか否かを判断する。初期設定を行わない場合には複写機 1 の処理を終了する。ステップ S 15 においてユーザパスワードの初期設定を行うと判断した場合には、ステップ S 16 に移行する。ステップ S 16 では、ホストコンピュータ 3 に対して通信を行い、パスワード設定要求の信号を送信する。ステップ S 17 では、ホストコンピュータ 3 との通信を終了する。ステップ S 18 では、ホストコンピュータ 3 から公衆回線 2 を介しての呼び出しがあったか否かを判断する。ホストコンピュータ 3 による呼び出しがあった場合には、ステップ S 19 に移行する。ステップ S 19 では、ホストコンピュータ 3 から送信されるパスワードを受信する。ステップ S 20 では、ステップ S 19 で受信したパスワードをパスワードメモリ 15 に格納する。この後ステップ S 2 に移行する。

【0018】ホストコンピュータ

複写機 1 からのパスワード設定要求があったときのホストコンピュータ 3 の動作を図 5 に示す。ステップ S 21 では、複写機 1 からのパスワード設定要求があったか否かを判断する。パスワード設定要求がない場合にはステップ S 25 に移行する。ステップ S 21 でパスワード設定要求があったと判断すると、ステップ S 22 に移行する。ステップ S 22 では該当する複写機 1 の回線番号を記憶装置 28 から読み出し、この回線番号に対する通話をモデム 27 を介して行う。ステップ S 23 では、ステップ S 22 で読み出した回線番号の複写機 1 と正常に通話ができたか否かを判断する。正常な通話が行えなかった場合には、ステップ S 25 に移行する。ステップ S 23 において正常な通話に成功したと判断した場合には、ステップ S 24 に移行する。ステップ S 24 では通話に成功した複写機 1 に対し、パスワード設定の信号を送信する。ステップ S 25 では他の処理を行う。

【0019】本実施例においては、パスワードメモリ 15 がメインスイッチ 18 を介さずに電源部に直接接続されており、複写機の電源ケーブルが所定の電源部から切り離されるとパスワードメモリ 15 内の記憶内容は消滅してしまう。したがって、パスワードメモリ 15 内に格納されているユーザパスワードも電源ケーブルの離脱に伴って消滅し、再度電源ケーブルが電源部に接続されても、ステップ S 6 で照合するためのユーザパスワードがなく、複写機の動作を停止したままとなる。したがって

盗難等により不正に複写機が移動された場合には、再度パスワードの設定を行うまでは複写動作が許可されず、不正な複写物の製造を防止できる。

【0020】また、所定回数以上の一致しないパスワードの入力に対して、パスワードメモリ 15 内に記憶されたユーザパスワードを消去してしまう構成であるため、セキュリティ効果が高い。

【0021】

【発明の効果】本発明に係る複写機管理装置では、パスワードメモリが揮発性の記憶手段で構成されており、複写機の電源ケーブルが所定の電源部に接続されているときのみパスワードメモリ用電源部により電源バックアップが行われている。したがって、複写機を不当に移動させて、電源ケーブルが一旦電源部から切り離された場合には、パスワードメモリ内に記憶されているユーザパスワードが消滅してしまう。したがって、不当に複写機を移動させて、不正な複写物の作成を行うことを防止できる。

【0022】パスワードメモリが、回線を介して接続されたホストコンピュータから設定されるユーザパスワードを記憶するように構成された場合には、停電等によってパスワードメモリ内の記憶内容が失われた場合にも、正当なユーザによる申告があれば、ホストコンピュータから新たにユーザパスワードを設定することが容易であり各種事故等に対しても対応することが可能となる。

【図面の簡単な説明】

【図 1】本発明の一実施例の概略構成図。

【図 2】その複写機の概略構成を示す制御ブロック図。

【図 3】そのホストコンピュータの概略構成を示す制御ブロック図。

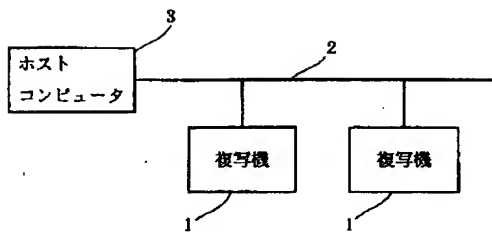
【図 4】複写機の制御フローチャート。

【図 5】ホストコンピュータの制御フローチャート。

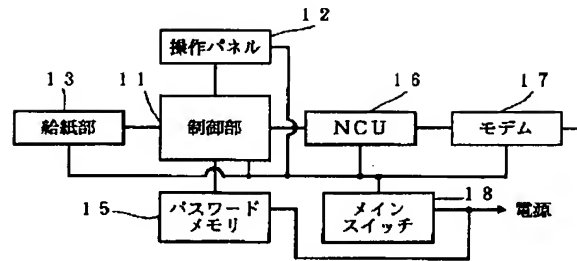
【符号の説明】

- 1 複写機
- 2 公衆回線
- 3 ホストコンピュータ
- 11 制御部
- 12 操作パネル
- 13 給紙部
- 15 パスワードメモリ
- 16 NCU
- 17 モデム
- 18 メインスイッチ

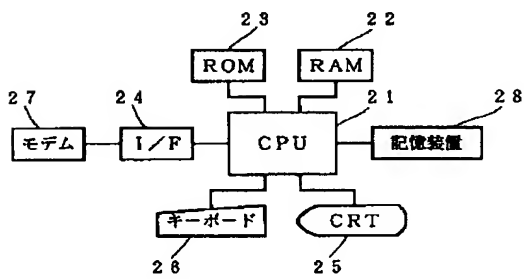
【図 1】



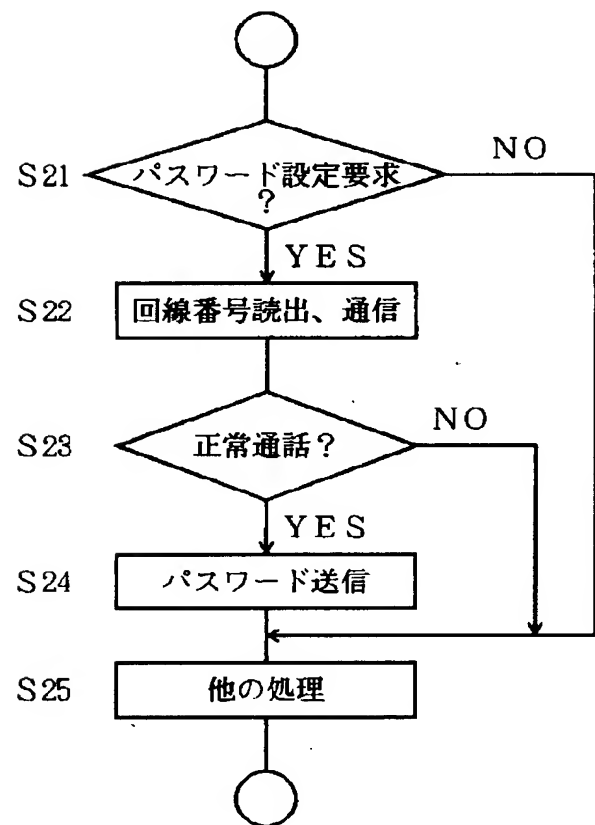
【図 2】



【図 3】



【図 5】



【図 4】

